Plan de Garantía de Seguridad

Infomaniak Network

Resumen

Resumen 2
1. Historial 5
2. Acerca de este documento 6
3. Introducción 7
3.1. Objeto del documento 7
3.2. Ámbito de aplicación 7
3.3. Evolución 7
3.4. Definiciones 7
4. Buenas prácticas 8
5. Gestión de riesgos 8
6. Política de Seguridad de la Información 8
7. Organización de la Seguridad de la Información 9
7.1. Funciones y responsabilidades 9
7.2. Gobernanza 9
7.3. Relaciones con los organismos y las autoridades 10
7.4. Vigilancia y seguridad 10
8. Seguridad de los recursos humanos 10
8.1. Contratación 10
8.2. Gestión de la confidencialidad 10
8.3. Sensibilización en materia de seguridad 11
8.4. Carta Informática 11
8.5. Competencias y formación 11
8.6. Finalización del contrato 12
9. Gestión de activos 12
9.1. Inventario 12
9.2. Licencias de software 12
9.3. Identificación y clasificación de los activos 12
9.4. Actualizaciones, antivirus y cifrado de medios 12
9.5. Nomadismo 13
9.6. Gestión de dispositivos y equipos extraíbles 13
9.7. Eliminación 13
10. Control de acceso y gestión de identidades 14
10.1. Política de contraseñas 14
10.2. Gestión de derechos 14
10.3. Revisión de los derechos 14
10.4. Eliminación del acceso 15
11. Criptografía 15

11.1. Uso de la criptografía 15
11.2. Uso de protocolos cifrados 15
11.3. Movilidad 15
12. Seguridad física y ambiental 15
12.1. Localización 15
12.2. Centros de datos 15
12.2.1. Seguridad física de las instalaciones y control de acceso 15
12.2.2. Seguridad de los equipos 16
12.2.3. Sistema de detección, de alarma y de extinción automática 16
12.3. Oficinas 16
12.3.1. Seguridad física de las instalaciones y control de acceso 16
12.4. Despacho vacío y pantalla en blanco 16
13. Seguridad operacional 17
13.1. Vigilancia de la ciberseguridad 17
13.2. Datos 17
13.2.1. Clasificación de los datos 17
13.2.2. Cifrado de los datos 17
13.2.3. Integridad de los datos 17
13.3. Gestión de los cambios 17
13.4. Protección contra malware 18
13.5. Política de copia de seguridad 18
13.6. Registro 18
13.7. Sincronización de relojes 18
13.8. Supervisión 19
13.8.1. Principios 19
13.8.2. Guardias 19
14. Seguridad de las comunicaciones 19
14.1. Arquitectura técnica 19
14.2. Internet 19
14.3. Redes Wi-Fi 19
14.4. Equipo de seguridad 20
14.4.1. Cortafuegos 20
14.4.2. IDS 20
14.4.3. Anti-DDoS 20
15. Adquisición, desarrollo y mantenimiento de los sistemas de información 20
15.1. Ciclo de vida de desarrollo seguro 20
15.2. Separación de los entornos de desarrollo, pruebas y operaciones 21
16. Relación con los proveedores 21
17. Gestión de vulnerabilidades e incidentes 21
17.1. Gestión de vulnerabilidades 21

17.2. Análisis de vulnerabilidades 22
17.3. Programa de bug bounty 22
17.4. Gestión de incidentes de seguridad 22
17.5. Gestión de crisis 22
18. Gestión de la continuidad del negocio 23
18.1. Continuidad del control 23
18.2. PCA y Resiliencia 23
18.3. Evaluación del impacto en la actividad 23
18.4. RPO y RTO 23
18.5. Plan de pruebas 24
19. Cumplimiento 24
19.1. Normas y reglamentos 24
19.1.1. ISO 27001 24
19.1.2. LPD y RGPD 24
19.2. Auditoría 24
19.2.1. Auditoría interna 24
19.2.2. Auditoría externa 25
19.2.3. Auditoría técnica 25
19.2.4. Auditoría de clientes 25

1. Historial

Fecha	Autoría	Función	Naturaleza de la modificación
13.05.2025	Johann Laqua	RSSI	Cambio del logotipo de la empresa, actualización de los capítulos sobre seguridad física, adición de un capítulo sobre definiciones
19.04.2024	Johann Laqua	RSSI	Finalización del documento para su primera publicación
14.02.2024	Johann Laqua	RSSI	Primera versión del documento

2. Acerca de este documento

El objetivo de este documento es presentar el Plan de Garantía de Seguridad de Infomaniak Network SA.

3. Introducción

3.1. Objeto del documento

El presente documento establece nuestro Plan de Garantía de Seguridad (PAS), que puede adjuntarse a nuestros contratos con nuestros clientes. Este plan define los compromisos asumidos por Infomaniak Network para responder a los requisitos contractuales en materia de Seguridad de los Sistemas de Información (SSI). Estos tienen por objeto:

- Garantizar la protección de los recursos de los sistemas de información utilizados en la prestación de servicios acordados contractualmente;
- Proteger a nuestros clientes de cualquier daño que pueda resultar de la indisponibilidad de dichos recursos, así como de cualquier violación de su integridad o confidencialidad.

Nuestro Plan de Garantía de Seguridad (PAS) detalla las diferentes disposiciones de seguridad, incluidas las medidas físicas, organizativas, de procedimiento y técnicas que hemos implementado.

3.2. Ámbito de aplicación

Este documento se refiere a los servicios gestionados por los equipos de Infomaniak Network, así como a sus actividades.

3.3. Evolución

Cualquier cambio en el Plan de Garantía de Seguridad (PAS) dará lugar a una nueva versión de este documento. Los cambios realizados se registran y fechan en el historial de versiones incluido en el documento.

El Plan de Garantía de Seguridad (PAS) es revisado al menos una vez al año por los responsables de cumplimiento y seguridad de los sistemas de información y aprobado por la dirección.

3.4. Definiciones

RSSI: Responsable de la seguridad de los sistemas de información
ISO: Organización Internacional de Normalización
EBIOS: Expresión de las necesidades y determinación de los objetivos de seguridad
Red team: Equipo de seguridad centrado en ejercicios y pruebas de seguridad ofensiva con personas de diferentes departamentos
ASDPO: Asociación Suiza de Responsables de Protección de Datos
NCSC: National Cyber Security Centre
CERT: Equipo de respuesta a emergencias informáticas
RR. HH.: Recursos Humanos

HTTPS: Protocolo seguro de transferencia de hipertexto
SSL: Capa de sockets seguros
IMAPS: Protocolo seguro de acceso a mensajes de Internet
SMTPS: Protocolo simple de transferencia de correo seguro
POP3S: Protocolo de oficina de correos versión 3
IDS: Sistema de detección de intrusiones
DDoS: Ataque de denegación de servicio distribuido
CVE: Vulnerabilidades y exposiciones comunes
PCA: Plan de continuidad de la actividad
RPO: Objetivo de punto de recuperación
RTO: Objetivo de tiempo de recuperación
LPD: Ley Federal de Protección de Datos
RGPD: Reglamento General de Protección de Datos

4. Buenas prácticas

La seguridad de Infomaniak Network está gestionada por un comité de seguridad, así como por un equipo de cumplimiento conforme a las normas ISO 27001 para toda la empresa. Infomaniak Network cuenta con la certificación ISO 27001:2022 en los siguientes ámbitos y actividades:

Desarrollo y suministro de infraestructura en la nube, servicios web, aplicaciones, atención al cliente, mantenimiento operativo de centros de datos.

5. Gestión de riesgos

Infomaniak Network ha formalizado una evaluación escrita de los riesgos que cubre todo el ámbito de aplicación del plan de garantía de seguridad, aplicando una metodología documentada que garantiza la reproducibilidad y la comparabilidad del proceso.

Este proceso de evaluación de riesgos incluye el análisis, la gestión y los planes de mitigación de riesgos, que dan lugar a medidas y proyectos concretos.

Además, Infomaniak Network se apoya en métodos ampliamente reconocidos como EBIOS RM para gestionar los riesgos en el marco de su sistema de gestión de la seguridad de la información (SMSI).

6. Política de Seguridad de la Información

Infomaniak Network tiene una Política de Seguridad que se encuentra en la siguiente dirección: https://www.infomaniak.com/documents/politique_SI_EE_es.pdf

Este documento establece claramente nuestros compromisos y objetivos con respecto a la seguridad de la información.

7. Organización de la Seguridad de la Información

Para estructurar nuestro enfoque de la seguridad de los sistemas de información (SSI), hemos implementado varias herramientas complementarias: un organigrama específico de SSI, una política interna de seguridad de los sistemas de información (PSSI) y un sistema de gestión de la seguridad de la información (SMSI). Estos elementos son esenciales para garantizar la aplicación rigurosa y coherente de nuestros procedimientos de seguridad.

7.1. Funciones y responsabilidades

Se han definido y asignado responsabilidades en materia de seguridad.

Infomaniak Network ha nombrado a un Chief Information Security Officer (CISO). Esta persona supervisa todas las medidas técnicas y organizativas implementadas en el marco de nuestra estrategia global de seguridad de la información.

Un comité de seguridad, compuesto por los responsables de los diferentes departamentos y equipos técnicos de la empresa, se reúne semanalmente para reuniones SOC (Security Operations Center) para discutir temas relacionados con la seguridad de la información.

Bajo la supervisión del CISO, un equipo Red Team realiza pruebas de seguridad en los productos y pruebas de ingeniería social entre los empleados de la empresa.

7.2. Gobernanza

Se ha creado un equipo dedicado a la gobernanza a nivel estratégico y operacional.

El equipo se reúne periódicamente para supervisar las cuestiones relacionadas con la seguridad de los sistemas de información. Las actas de esas reuniones se conservan en condiciones de seguridad.

7.3. Relaciones con los organismos y las autoridades

Infomaniak Network es miembro de una asociación profesional (ASDPO) y mantiene relaciones con las autoridades (NCSC y Cyber Security Hub) para los avances en el ámbito de la seguridad de la información.

7.4. Vigilancia y seguridad

Se ha establecido y se lleva a cabo una vigilancia de la seguridad, técnica y legal, dentro de la actividad. Permite

prevenir los riesgos específicos de las actividades de Infomaniak Network.

Infomaniak Network se apoya en una asociación con una empresa especializada en ciberseguridad para vigilar en la dark web los activos sensibles que están bajo su responsabilidad.

8. Seguridad de los recursos humanos

8.1. Contratación

Nuestro departamento de RR. HH. aplica un procedimiento de contratación para cada candidato, con medidas de seguridad proporcionales al nivel de clasificación de cada empleado y a los riesgos identificados.

Se realizan las siguientes comprobaciones:

- Comprobación de la identidad del candidato
- Verificación de las competencias del puesto
- Verificación de las referencias del candidato
- Verificación de antecedentes penales
- Verificación exhaustiva de antecedentes para candidatos de alto nivel de seguridad

8.2. Gestión de la confidencialidad

Los contratos de trabajo establecen claramente las responsabilidades del personal en materia de seguridad de la información.

Una cláusula de confidencialidad, extraída de las condiciones generales del contrato de trabajo, obliga al personal a respetar estrictamente la confidencialidad de los datos sensibles y privados a los que tenga acceso en el marco de sus funciones en Infomaniak. Cualquier violación de esta cláusula entraña consecuencias para el infractor.

Además, se ha establecido un proceso disciplinario oficial que se ha comunicado a todo el personal y a otras partes interesadas pertinentes. Este proceso prevé sanciones adecuadas para cualquier persona que infrinja la política de seguridad de la información.

8.3. Sensibilización en materia de seguridad

Realizamos sesiones de integración de seguridad para verificar el cumplimiento de las estaciones de trabajo, al tiempo que educamos a los colegas sobre los riesgos de seguridad de los sistemas de información (SSI) y de nuestros procedimientos de seguridad física e informática.

Durante estas sesiones, también presentamos documentos importantes como nuestra Política de Seguridad de la Información (PSI) y nuestras Pautas Generales de Seguridad.

Todos los años elaboramos un programa de concienciación que utiliza diversos instrumentos de evaluación sobre distintos temas relacionados con la seguridad y la ciberseguridad. Esto incluye campañas de phishing e ingeniería social, entre otras.

Se realizan varias comunicaciones a los empleados por correo electrónico con el fin de sensibilizarlos sobre los riesgos de seguridad de la información, la protección de datos, los riesgos cibernéticos y las actualizaciones de nuestro sistema de gestión de la seguridad de la información.

8.4. Carta Informática

Infomaniak Network dispone de Directrices Generales en materia de Seguridad, equivalentes a una Carta informática, que se actualizan periódicamente y se comunican a todos los miembros de nuestra empresa.

Desde el momento de su contratación, y todos los años, se comprometen solemnemente a respetarlas; de lo contrario, podrían ser objeto de sanciones disciplinarias.

8.5. Competencias y formación

Cada año, durante las entrevistas individuales, el Departamento de Recursos Humanos realiza una encuesta entre los empleados para evaluar sus necesidades de formación. A continuación se establece un programa anual de formación para determinar los cursos necesarios para solucionar:

- las deficiencias en las competencias de un empleado, equipo o departamento;
- las necesidades de desarrollo continuo de las competencias.

Las formaciones propuestas pueden impartirse internamente o a través de proveedores externos.

A lo largo del año, los delegados o expertos en ciberseguridad ofrecen una serie de cursos de formación técnica, así como informes y estadísticas trimestrales sobre las vulnerabilidades que podrían afectar a nuestros sistemas, con el fin de mejorar las competencias de nuestro personal.

8.6. Finalización del contrato

Se ha establecido un procedimiento de salida o rescisión del contrato que se ha comunicado a todos los responsables afectados de la empresa. Este procedimiento tiene por objeto garantizar que el empleado ya no tenga acceso físico ni informático al sistema de información de la empresa.

9. Gestión de activos

9.1. Inventario

Infomaniak Network elabora inventarios de activos esenciales y bienes de apoyo. Estos últimos se identifican en nuestro Sistema de Gestión de la Seguridad de la Información (SMSI) y en nuestras evaluaciones de riesgos.

Revisamos estos activos cada año a través del SMSI y los actualizamos a través de procesos automatizados de acuerdo con los requisitos de los diferentes equipos internos.

9.2. Licencias de software

Infomaniak Network se compromete a garantizar el uso de licencias válidas para los programas de terceros en sus equipos internos y adopta las medidas necesarias para proteger los derechos de propiedad intelectual.

9.3. Identificación y clasificación de los activos

Los activos están segmentados y claramente identificados mediante una nomenclatura y una convención de denominación establecidas por los equipos internos. Se establecen controles permanentes y anuales para garantizar la legitimidad del acceso, la restricción del acceso no autorizado y la fiabilidad del inventario.

Los datos se clasifican de acuerdo con las necesidades de seguridad de la información de la organización, teniendo en cuenta los requisitos de confidencialidad, integridad y disponibilidad, así como las principales preocupaciones de las partes interesadas.

9.4. Actualizaciones, antivirus y cifrado de medios

El Director de Seguridad de Sistemas de Información (RSSI) supervisa la protección central de los activos de la empresa, incluidos los puestos de trabajo de los empleados, contra virus y malware. Una estrategia de defensa contra estas amenazas se ve reforzada por una formación adecuada de los usuarios.

La seguridad de los medios de almacenamiento internos y extraíbles está garantizada por un proceso de cifrado configurado y supervisado.

Los indicadores clave de rendimiento (KPI) se supervisan periódicamente para verificar el cumplimiento y la protección de los activos.

9.5. Nomadismo

Para garantizar la seguridad de la información durante el teletrabajo, se han tomado diversas precauciones. Se han elaborado directrices específicas sobre el teletrabajo, que se

han puesto a disposición del personal. Es obligatorio utilizar una red privada virtual (VPN) segura para conectarse a los recursos de la organización desde el exterior.

Además, el uso de dispositivos personales («Bring Your Own Device» o BYOD) no está permitido en este contexto.

9.6. Gestión de dispositivos y equipos extraíbles

Se han elaborado y difundido directrices sobre el uso de medios extraíbles, que son bien conocidas por el personal. Estas instrucciones incluyen normas estrictas para su uso con el fin de minimizar los riesgos potenciales y recomendaciones para garantizar su protección.

Por ejemplo, puede pedirse que se cifren los medios extraíbles que contengan datos confidenciales o críticos, o que se restrinja su uso a determinadas circunstancias.

9.7. Eliminación

Se ha elaborado y se aplica una política de reciclado de equipos y eliminación de activos para gestionar los activos sensibles de la empresa.

El objetivo de este procedimiento es proporcionar instrucciones claras sobre el tratamiento de todo tipo de equipo que contenga datos confidenciales. Esto incluye reglas para garantizar la destrucción segura de los datos antes de la transferencia o eliminación del material, a fin de evitar su recuperación posterior.

10. Control de acceso y gestión de identidades

10.1. Política de contraseñas

Los empleados deben aplicar nuestra política de gestión de contraseñas para garantizar la seguridad de nuestras cuentas y datos durante todo su ciclo de vida.

También nos comprometemos a informar a nuestros usuarios sobre los requisitos específicos relacionados con nuestra política de contraseñas, teniendo en cuenta sus competencias, su función y la sensibilidad de los recursos a los que pueden acceder.

Estas son algunas de las buenas prácticas recomendadas en nuestra política de contraseñas:

- Obligación de utilizar un gestor de contraseñas autorizado para generar y almacenar contraseñas seguras;
- Crear contraseñas seguras con al menos 12 caracteres alfanuméricos y especiales;
- Evitar el uso de términos de uso común o fácilmente adivinables;
- Nunca compartir la contraseña con otra persona ni reutilizarla en varias cuentas;
- Configurar la autenticación multifactor siempre que sea posible;

Recomendamos encarecidamente a todos nuestros usuarios que sigan estrictamente estos consejos para ayudar a mantener un alto nivel de seguridad dentro de nuestra organización.

10.2. Gestión de derechos

Esta asignación de acceso se organiza por departamento, concediendo únicamente los permisos necesarios en función de las tareas asignadas a cada persona.

Todas las solicitudes de autorización se presentarán a través de canales internos predefinidos y se aprobarán tras un examen minucioso.

10.3. Revisión de los derechos

El RSSI y los delegados de seguridad revisan anualmente los derechos de acceso.

Todos los años se llevan a cabo controles de seguridad de los servicios internos y externos, los ordenadores de sobremesa, los accesos a las redes inalámbricas y Wi-Fi.

La gestión avanzada del acceso interno se comprueba automáticamente y anualmente a través de herramientas internas.

10.4. Eliminación del acceso

La eliminación del acceso de los empleados de Infomaniak Network está relacionada con el proceso de RR.HH. de gestión de entradas y salidas. Este proceso de salida se supervisa rigurosamente mediante instrumentos internos dedicados, dirigidos por funcionarios designados para tomar las medidas necesarias.

11. Criptografía

11.1. Uso de la criptografía

Se han definido y aplican normas para el uso eficaz de la criptografía, incluida la gestión de claves criptográficas.

Infomaniak Network ha elaborado y aplica una Política de control criptográfico y de cifrado, que ha sido difundida y que es conocida por todo el personal.

11.2. Uso de protocolos cifrados

Infomaniak Network y sus colaboradores velan por utilizar protocolos de red seguros con la mayor frecuencia posible, tanto en las redes públicas como en Internet, así como en su red interna. Por ejemplo, promovemos el uso de HTTPS para la navegación web, IMAPS, SMTPS o POP3S para la mensajería y SSH (Secure Shell) para las operaciones de administración del sistema.

11.3. Movilidad

Los empleados de la empresa Infomaniak Network utilizan únicamente sus ordenadores portátiles para conectarse de forma remota a la red interna de seguridad de la empresa.

12. Seguridad física y ambiental

12.1. Localización

Los centros de datos de Infomaniak Network están situados exclusivamente en Suiza y son propiedad de la empresa en su totalidad.

12.2. Centros de datos

12.2.1. Seguridad física de las instalaciones y control de acceso

Los locales se vigilan constantemente mediante un sistema de cámaras de videovigilancia para impedir el acceso físico no autorizado.

El acceso a los centros de datos y servidores está protegido por varias compuertas y un sistema electrónico de control de acceso con identificación biométrica. Para aumentar aún más la seguridad del centro de datos, cada área y pasillo que da servicio a los racks está equipada con un sistema de reconocimiento facial.

El acceso a las salas de servidores está restringido a un número limitado de empleados de la empresa, especialmente cualificados y autorizados en áreas de trabajo segmentadas según las necesidades específicas de los diferentes equipos.

12.2.2. Seguridad de los equipos

Todos los centros de datos cuentan con las certificaciones ISO 27001, ISO 14001 y cuentan con redundancia n+1 en alimentación, red troncal de fibra óptica, refrigeración, generadores e inversores para garantizar el funcionamiento ininterrumpido de la infraestructura técnica.

12.2.3. Sistema de detección, de alarma y de extinción automática

Nuestras sedes están monitoreadas y totalmente equipadas con sistemas de detección de incendios. Nuestros sistemas de extinción de incendios, calibrados para cada tipo de entorno de un centro de datos, garantizan la extinción automática de incendios en zonas en las que podría iniciarse un incendio. Estos sistemas se encuentran en los lugares en los que hay equipos eléctricos, como inversores, baterías o cuadros de distribución. Este dispositivo de vigilancia funciona permanentemente y es sometido a pruebas periódicas.

12.3. Oficinas

12.3.1. Seguridad física de las instalaciones y control de acceso

Las oficinas de la sede central de Infomaniak Network están equipadas con puertas de cierre automático, a las que solo se puede acceder mediante un sistema de identificación y reconocimiento facial: se realizan controles físicos de acceso periódicos.

Se han instalado cámaras de vigilancia en los pasillos y en las zonas comunes del edificio, incluso en las inmediaciones de los espacios de trabajo de los empleados.

12.4. Despacho vacío y pantalla en blanco

Se ha establecido una política de despacho vacío y pantalla en blanco, que se ha comunicado a todos los empleados. Incluye instrucciones detalladas sobre el bloqueo de las pantallas, la gestión adecuada de los documentos impresos y digitales, el uso de pizarras blancas y la destrucción segura de documentos confidenciales.

13. Seguridad operacional

13.1. Vigilancia de la ciberseguridad

La información sobre las amenazas a la seguridad de la información se recopila, analiza y procesa con el fin de generar información sobre dichas amenazas.

Contamos con un servicio de terceros que nos permite supervisar las actividades y amenazas en la Dark Web.

La búsqueda de estas amenazas potenciales se lleva a cabo mediante palabras clave y términos específicos predeterminados, incluidos los relacionados con:

- La exposición de los empleados;
- La supervisión de la marca y los nombres de dominio;
- El seguimiento de la Dark Net;
- La exploración de la deep web y el descubrimiento de activos.

13.2. Datos

13.2.1. Clasificación de los datos

La información se clasifica de acuerdo con las necesidades de seguridad de la información de la organización, basándose en los requisitos de confidencialidad, integridad, disponibilidad y requisitos importantes de las partes interesadas.

13.2.2. Cifrado de los datos

Los datos se protegen durante su transferencia entre las estaciones de trabajo de los empleados, los clientes y el sistema de información de Infomaniak Network mediante el uso de protocolos de cifrado descritos en el capítulo 11 de este documento.

13.2.3. Integridad de los datos

Infomaniak Network se compromete a proteger los datos de sus clientes estableciendo procedimientos, medidas técnicas y protocolos seguros para evitar cualquier alteración, ya sea voluntaria o accidental. Esto incluye salvaguardias sólidas para la transmisión y el mantenimiento de la información confidencial.

13.3. Gestión de los cambios

Nuestra política de gestión de cambios ofrece a los usuarios un conjunto de procedimientos operativos bien documentados y controles estrictos sobre los mismos. Incluye:

- El marco de los cambios, definiendo claramente su alcance y sus objetivos;
- Las directrices para la aplicación de los cambios, incluidos los criterios de aceptación y las normas de seguridad;
- La planificación detallada de los cambios, incluida la identificación de los riesgos potenciales y los planes de contingencia adecuados;
- El control estricto de los cambios, con una trazabilidad completa de todos los cambios realizados en el sistema;
- Procesos claros y fáciles de seguir para las actualizaciones periódicas del sistema, lo que garantiza una estabilidad y un rendimiento óptimos.

13.4. Protección contra malware

La protección contra los programas maliciosos se implementa y se refuerza mediante una concienciación adecuada de los usuarios. El parque informático de las estaciones de trabajo se supervisa mediante un programa antivirus centralizado y comprobaciones periódicas. Se establecen indicadores que se revisan durante las reuniones de seguridad.

13.5. Política de copia de seguridad

Existe una política de copia y seguridad de los datos, que establece directrices claras para copiar y restaurar la información de acuerdo con los activos identificados en nuestro sistema de información. Esta política especifica el período de conservación, la frecuencia, el tipo de cifrado y los protocolos de prueba que se deben seguir.

Gracias a estas medidas, podemos garantizar la protección y recuperación efectivas de nuestros datos importantes.

13.6. Registro

Se generan, mantienen, protegen y analizan registros que recogen actividades, excepciones, fallos y otros eventos pertinentes.

13.7. Sincronización de relojes

Los relojes de los sistemas de procesamiento de la información utilizados por la organización se sincronizan con las fuentes de tiempo aprobadas.

Infomaniak Network dispone de sus propios servidores de referencia temporal, que permiten a todos los aparatos y servidores beneficiarse de una sincronización temporal precisa. Este servicio también es accesible para el público y se pone a disposición tanto de los clientes como de los no clientes.

13.8. Supervisión

13.8.1. Principios

Todos los servicios y sistemas administrados por Infomaniak Network son objeto de un estrecho seguimiento. Nuestras herramientas de supervisión se basan en protocolos estándar, así como en autómatas diseñados específicamente para recopilar datos de todas las fuentes de control.

En caso de fallo, se emiten alertas en tiempo real para todos los servicios supervisados.

Estas alertas también pueden enviarse por SMS a los equipos de guardia durante las horas fuera de servicio.

13.8.2. Guardias

El equipo de guardia supervisa e interviene las 24 horas del día, los 7 días de la semana, en el sistema de información (SI) de Infomaniak Network. Este equipo está estructurado en diferentes niveles y reúne a especialistas de diversos equipos de producción, cubriendo así todas las áreas de especialización.

14. Seguridad de las comunicaciones

14.1. Arquitectura técnica

La infraestructura que presta los servicios de Infomaniak Network está compartimentada y estructurada en varias zonas de seguridad separadas. Este diseño ofrece una seguridad mejorada, escalable y adaptada a los requisitos actuales y futuros. Los grupos de servicios de información, usuarios y sistemas de información están aislados dentro de las redes

internas de la organización, lo que garantiza un alto nivel de protección contra posibles amenazas externas o internas.

14.2. Internet

Infomaniak Network dispone de sus propias direcciones IP públicas, así como de varias conexiones a Internet de diferentes proveedores. Esto permite a la empresa garantizar un nivel óptimo de servicio a sus clientes y empleados, incluso en caso de fallo de un proveedor. Además, todas las prestaciones gestionadas por Infomaniak se benefician de una redundancia, lo que garantiza su continuidad.

14.3. Redes Wi-Fi

Las redes Wi-Fi de Infomaniak están segmentadas en función de sus usos específicos, como redes Wi-Fi de invitados, empleados, preproducción, etc., con un control de acceso basado en la gestión de derechos. Además, los puntos de acceso Wi-Fi están protegidos para evitar el acceso no autorizado.

14.4. Equipo de seguridad

14.4.1. Cortafuegos

En Infomaniak, se instalan cortafuegos entre cada zona de seguridad y cada zona de aplicación. Por ejemplo, los flujos entrantes procedentes del exterior tienen que atravesar varios niveles de cortafuegos antes de llegar al servicio solicitado, lo que garantiza una mayor protección contra amenazas potenciales.

14.4.2. IDS

Se han instalado sondas IDS en puntos clave de la red Infomaniak para analizar los flujos de entrada y salida del sistema de información. Estas sondas se encargan de detectar actividades sospechosas o anómalas, así como tráfico malicioso, e informar inmediatamente a los equipos de producción. Para ello, las sondas reciben actualizaciones periódicas de firmas de ataques de nuestro proveedor especializado en ciberseguridad. La instalación y el mantenimiento de estos dispositivos son responsabilidad del equipo de seguridad de producción.

14.4.3. Anti-DDoS

Infomaniak implementa una protección anti-DDoS adecuada para cada una de las tecnologías que explota, garantizando así la defensa de todas sus plataformas e infraestructuras frente a este tipo de ciberamenazas. Al hacerlo, se propone mantener un alto nivel de disponibilidad y resiliencia de sus servicios, en beneficio de sus clientes y su personal.

15. Adquisición, desarrollo y mantenimiento de los sistemas de información

15.1. Ciclo de vida de desarrollo seguro

Se han establecido y aplican normas de seguridad, buenas prácticas y sentido común para garantizar el desarrollo seguro de programas informáticos y sistemas. Entre esos principios figuran los siguientes:

- Auditoría y registro de acciones
- Formación de los desarrolladores en seguridad
- Lucha contra el malware
- Pruebas de seguridad de las aplicaciones
- Pruebas de conformidad del sistema
- Seguridad de las aplicaciones web del lado del cliente y del servidor
- Seguridad de las aplicaciones móviles
- Criptografía

El personal del departamento de desarrollo es consciente de los riesgos de seguridad de las aplicaciones y de los estándares establecidos por el Open Web Application Security Project (OWASP).

Además, hemos implementado una política de supervisión y control del desarrollo externo que recomienda las modalidades de ejecución, las medidas de seguridad existentes y las instrucciones obligatorias para la gestión de registros, la gestión de acceso, la gestión del código fuente y las pruebas de seguridad durante el ciclo de desarrollo.

15.2. Separación de los entornos de desarrollo, pruebas y operaciones

Nuestras redes e infraestructuras de desarrollo cuentan con aislamiento físico e informático de acuerdo con los servicios prestados. También establecemos una separación entre los diversos entornos de aplicación, como los dedicados al desarrollo, las pruebas, la preproducción y la producción.

En concreto, el entorno de desarrollo está estrictamente restringido y solo es accesible para los desarrolladores a través de nuestra red interna altamente segura.

16. Relación con los proveedores

Hemos implementado procesos y procedimientos para gestionar los riesgos potenciales para la seguridad de la información derivados del uso de nuestros productos o servicios por parte de determinados proveedores.

Además, nos aseguramos de establecer y acordar los requisitos de seguridad de la información adecuados con cada uno de nuestros proveedores.

Así mismo, periódicamente revisamos, evaluamos y gestionamos de forma proactiva los cambios en las prácticas de seguridad de la información de nuestros respectivos proveedores de bienes y servicios.

17. Gestión de vulnerabilidades e incidentes

17.1. Gestión de vulnerabilidades

Se ha implementado un flujo de trabajo por parte de los equipos de producción para gestionar las vulnerabilidades de tipo CVE utilizando herramientas internas y de vigilancia tecnológica.

Diversas herramientas internas permiten el seguimiento, la supervisión y la exploración automatizada de vulnerabilidades que puedan afectar a nuestros sistemas de información.

Se ha establecido un acuerdo de nivel de servicios (SLA) interno para tramitar las notificaciones de vulnerabilidades, con plazos de respuesta ajustados a la gravedad de las deficiencias detectadas.

17.2. Análisis de vulnerabilidades

Los análisis se llevan a cabo regularmente en varios rangos de direcciones IP de Infomaniak especificados por nosotros. Recibimos alertas a través de un cuadro de mando cuando se detectan vulnerabilidades, y programamos planes de acción para corregir rápidamente las vulnerabilidades descubiertas.

17.3. Programa de bug bounty

Colaboramos activamente con una comunidad de investigadores y hackers éticos para ofrecer a nuestros clientes el nivel óptimo de seguridad. Existe un programa público, así como programas privados, para probar todos los servicios ofrecidos a nuestros clientes.

Los denunciantes están protegidos adecuadamente, mientras que nuestros empleados tienen la oportunidad de notificar cualquier irregularidad sospechosa de forma confidencial y anónima en cualquier momento.

17.4. Gestión de incidentes de seguridad

Un procedimiento bien establecido de gestión de incidentes de seguridad define claramente las funciones, las responsabilidades, el proceso de selección, la comunicación, la respuesta y la mitigación, así como todo el flujo de trabajo necesario para garantizar una resolución completa del incidente.

En función de la gravedad y la naturaleza del evento, Infomaniak Network puede colaborar activamente con las autoridades competentes y coordinar el proceso de tratamiento de la incidencia con el fin de garantizar su resolución rápida y eficaz.

17.5. Gestión de crisis

Se ha formalizado un procedimiento específico de gestión de crisis. Este procedimiento describe los diferentes pasos que deben seguirse para resolver el incidente de la manera más eficaz posible y para comunicar de la mejor manera, tanto interna como externamente, la causa y los efectos.

18. Gestión de la continuidad del negocio

18.1. Continuidad del control

Se ha definido un plan de continuidad para la gestión y el control de los servicios y activos de la infraestructura de nuestros centros de datos.

18.2. PCA y Resiliencia

La continuidad de la actividad se tiene en cuenta desde la fase de diseño y arquitectura de los servicios gestionados por Infomaniak Network.

La redundancia entre nuestros centros de datos, así como la copia de seguridad en varios soportes y en varios de nuestros centros de datos, ayudan a garantizar la continuidad del negocio para nuestros clientes.

Las soluciones de recuperación ante desastres de nuestros servicios gestionados dependen de las arquitecturas técnicas y de software y se adaptan a cada oferta de negocio, dependiendo de las limitaciones específicas y de los equipos de producción.

18.3. Evaluación del impacto en la actividad

Se ha implementado una Evaluación de Impacto en la Actividad (BIA) con el objetivo de recopilar datos para planificar y gestionar eficazmente los incidentes de seguridad que afecten a los activos de nuestro sistema de información.

Este BIA ayuda a identificar las actividades y los recursos clave de la empresa, así como los diferentes niveles de gravedad asociados. También se han definido medidas específicas para garantizar la continuidad de la actividad en caso de incidente.

18.4. RPO y RTO

Infomaniak Network ha establecido una estrategia de continuidad teniendo en cuenta tres factores clave:

- El Tiempo de Interrupción Máximo Permisible (TMA), también conocido como Objetivo de Tiempo de Recuperación (OTR) u Recovery Time Objective (RTO);
- La Pérdida Máxima Aceptable de Datos (PMAD), también conocida como Objetivo de Punto de Recuperación (OPR) o Recovery Point Objective (RPO).
- Posibles impactos financieros y comerciales.

Cuando estos elementos son pertinentes, se consignan en la Evaluación de Impacto en la Actividad (BIA).

18.5. Plan de pruebas

Todos los años se elabora y aplica un plan de pruebas en el que se tienen en cuenta las situaciones de riesgo. Permite lo siguiente:

- Previamente: medir la eficacia del plan en relación con los objetivos de continuidad, mediante indicadores, auditorías, etc.
- Durante una crisis: supervisar los niveles de servicio realmente alcanzados y el funcionamiento de los procedimientos operativos previstos en el marco del PCA.
- A posteriori: establecer un plan de mejora.

19. Cumplimiento

19.1. Normas y reglamentos

19.1.1. ISO 27001

Los equipos de Infomaniak Network se basan en normas de seguridad reconocidas internacionalmente, como ISO 27001:2022 e ISO 27002:2022, como referencias para desarrollar y gestionar los servicios que ofrecen a sus clientes.

Estas normas proporcionan un marco sólido para garantizar la confidencialidad, la integridad y la disponibilidad de los datos sensibles, así como para garantizar una gestión eficaz de los riesgos de seguridad de la información.

19.1.2. LPD y RGPD

Infomaniak Network ha establecido una política de confidencialidad de los datos, que puede consultarse en su sitio web en la dirección siguiente:
https://www.infomaniak.com/es/ccgg/politica-de-confidencialidad

Además, se puede acceder a la política de uso de las cookies a través de este enlace:
https://www.infomaniak.com/es/ccgg/politica-uso-galletas

19.2. Auditoría

19.2.1. Auditoría interna

La supervisión de las actividades de seguridad en las zonas de certificación de Infomaniak Network está a cargo de consultores cualificados que trabajan bajo la supervisión del equipo de cumplimiento.

Los consultores examinan periódicamente los elementos relacionados con los ámbitos certificados, de conformidad con el plan de auditoría y la declaración de aplicabilidad de Infomaniak Network.

Los documentos de auditoría interna son confidenciales y no pueden divulgarse.

19.2.2. Auditoría externa

En el marco de la certificación ISO 27001:2022, Infomaniak Network es auditada anualmente por los organismos certificadores.

19.2.3. Auditoría técnica

Infomaniak Network recurre a expertos cualificados para llevar a cabo auditorías técnicas periódicas de su sistema de información y según las necesidades y para la producción de nuevos servicios.

19.2.4. Auditoría de clientes

Los clientes tienen la posibilidad de realizar pruebas de intrusión (pentest) en los servicios que utilizan, respetando estrictamente las condiciones especificadas en su contrato.

También deben tener en cuenta las limitaciones de los equipos internos, como la realización de pentests sólo durante las horas de oficina e informar a los equipos de producción con antelación.